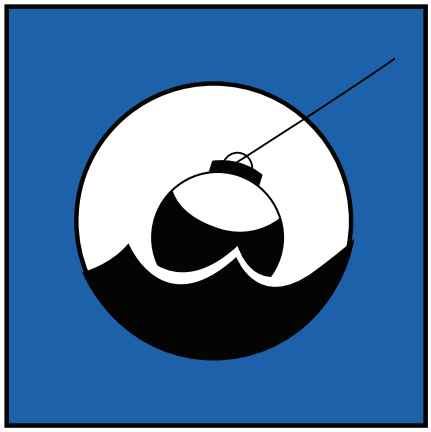
Federal Trade Commission



Roundtable Discussion on Phishing Education

A Staff Report by the Federal Trade Commission's
Division of Consumer and Business Education
and Division of Marketing Practices
July 2008

TABLE OF CONTENTS

I. Background and Overview

Phishing uses deceptive spam that appears to be coming from legitimate, well-known sources to trick consumers into divulging sensitive or personal information, such as credit card numbers, other financial data, or passwords, either through a reply email or a link to a copycat of the purported source's website. During the July 2007 Spam Summit of the Federal Trade Commission ("FTC"), panelists identified consumer and business education as a key tool for helping to reduce the number of consumers who fall victim to phishing scams.[1] Following the Summit, in a speech before the National Cyber Security Alliance, then FTC Chairman Deborah Platt Majoras announced that the agency would host a half-day workshop focused on revitalizing anti-phishing consumer and business education.[2]

The workshop was held April 1, 2008; approximately 60 experts from business, government, the technology sector, the consumer advocacy community, and academia met to discuss strategies to reach and teach consumers about phishing. The Bureau of Consumer Protection's Divisions of Consumer and Business Education and Marketing Practices hosted the event at the FTC's conference center. A copy of the agenda is attached.

Staff established and met three main goals for this workshop:

- to learn about organizations' methods for responding to phishing attacks and informing their customers about the attacks;

---

[1] The Spam Summit was held on July 11-12, 2007. The Spam Summit staff report, *Spam Summit: The Next Generation of Threats and Solutions, A Staff Report by the Federal Trade Commission's Division of Marketing Practices* (Nov. 2007), is available at http://www.ftc.gov/os/2007/12/071220spamsummitreport.pdf.

[2] A copy of Chairman Majoras's speech, *Maintaining Momentum in the Fight Against Identity Theft* (Oct. 2007), is available at: http://www.ftc.gov/speeches/majoras/071001ncsas.pdf.

- to identify opportunities to teach consumers about phishing, and to mobilize key players to seize these "teachable moments" to educate consumers about the risks of certain online behaviors and the rewards of others; and
- to develop an action plan to raise consumer awareness about phishing and change consumers' risky online practices.

The workshop featured two guided roundtable discussions, followed by a break-out session to discuss next steps. Between sessions, staff introduced and previewed three 60-second FTC videos on phishing, which now have been posted on these websites: www.onguardonline.gov, www.ftc.gov, and www.youtube/ftcvideos. OnguardOnline.gov is the federal government's website with information to help consumers be on guard against Internet fraud, secure their computers, and protect their personal information.

II. Next Steps

The roundtable discussion revealed that phishers' practices are dynamic and evolving. Phishing education requires collaboration among members of the anti-phishing community. Participants agreed there are untapped opportunities for teaching consumers and businesses about how to avoid phishing. Details about what participants learned and shared during the roundtable are discussed in greater detail in Section III. FTC staff look forward to following up with stakeholders to take the next steps identified during the workshop, including:

- **Developing a Task Force to Continue the Dialogue —** During the workshop, the National Cyber Security Alliance announced that it is forming a Task Force on phishing education, and asked attendees to participate. Most attendees agreed to be part of this group. FTC staff also plan to participate.

- **Using Landing Pages as "Teachable Moments" —** As part of their anti-phishing measures, some ISPs and other entities monitor websites and take down pages used for phishing. Several participants supported the idea of replacing these pages with landing pages containing educational messages so that users who click to the URL after the educational page is posted will learn that they could have clicked on a scam site and how to avoid that in the future. Some companies have already used educational landing pages with success. The Anti-Phishing Working Group has developed educational phishing landing pages and will translate them into various languages for use by domestic — as well as foreign — ISPs.
- **Mobilizing Participants to Disseminate New Consumer Education —** The FTC's new phishing videos were launched and several participants agreed to place the videos on their websites and distribute them through other channels.

III. Discussion Summary

A. First Session: Problem Overview

The first session began with a discussion of the impact of phishing on businesses and organizations. Participants discussed the phishing problem from their organization's perspective and addressed some of the challenges of educating computer users.

Laura Mather, Managing Director of Operational Policy for the Anti-Phishing Working Group, provided several observations. First, phishers seem to be using lesser-known brands more often than widely-known brands to dupe consumers. Second, phishers continue to be extremely nimble in their use of technology for subversive tactics. Illustrating this point, Marcus Jakobsson, a researcher with the Palo Alto Research Center and former professor of informatics at Indiana University, noted that some phishing emails are able to scan a user's browser history to identify

recent websites visited and, using this information, automatically configure themselves to take on the look of the recipient's financial institution, or of a financial institution that the recipient recently visited online. This type of phishing attack poses education challenges because consumers are likely to see fewer emails that appear to be from unfamiliar institutions, and more emails that appear to be from familiar ones.

Despite increasingly insidious trends in phishing attacks, many participants indicated that consumer confidence on the Internet is high, and that this trust makes many consumers unsafe. Citing a poll conducted by Zogby International, Max Weinstein of Harvard Law School's Berkman Center for Internet and Society, noted that while 88 percent of users feel safe using a personal computer to access the Internet and 84 percent believe they have the tools necessary to be safe on it, far fewer actually have such tools.

In addition, workshop participants believed that consumers generally under-report their vulnerability to phishing scams. That makes it difficult for organizations to grasp the true size of the problem. Under-reporting may result from consumers not being able to identify an email as a "phish" or not knowing whether they have been a victim of a "phish," because any connection between a phishing email and a later incident of identity theft or account misuse may not be apparent.

B. Second Session: Current Efforts to Fight Phishing Attacks and Educate Consumers

Most attendees reported that their organizations provide information to consumers about how to report phishing and have security information on their websites to help educate consumers about the practice. Among the tools that organizations use to mitigate phishing attempts are: 1) a personal image that a customer always sees when logging on that authenticates the site for the user, 2) a tagline on every email from the company explaining that they will never ask for

the customer's password or banking information, and 3) toolbars that warn customers whether a site is suspicious.

Many organizations work behind the scene — and screen — with ISPs to reduce the number of phishing emails delivered to their customers. Some of their practices are: 1) having authentication mechanisms at the domain level, 2) providing filters to keep phishing emails out of the customer's inbox, and 3) tagging all brand logos and images to reduce the time it takes to find spoofed sites. Representatives of ISPs noted that they usually work directly with organizations to alert them that their products are being used for phishing attempts.

C. Third Session: Developing a Plan to Increase Effective Consumer Education and Mobilize Key Players

During the break-out sessions, participants discussed potential elements of an action plan for phishing education. Participants were interested in continuing to work together to refine anti-phishing messages for consumers and businesses, working on strategies to reach consumers at the "teachable moment" (using, for example, security toolbars and informational landing pages), and developing new communications channels to raise awareness of online security. The National Cyber Security Alliance announced the formation of a task force on phishing education; the Anti-Phishing Working Group announced the intention to develop phishing landing pages; and several attendees committed to placing the FTC's new videos on their websites and otherwise promoting the videos.

Three key themes emerged during the break-out sessions:

- methods for refining the message;
- strategies for reaching the right people at the right time; and
- developing guidance for businesses.

1. Methods for Refining the Message

Participants agreed that anti-phishing messages should be reviewed and refined for simplicity, consistency, and positiveness. Many suggested that the government should focus on coordinating education efforts, and that making anti-phishing messages consistent requires a concerted effort.

a. Linking anti-phishing messages to identity theft

Participants noted that continuing to link anti-phishing messages to identity theft is a good practice because consumers are already aware of the dangers of identity theft. Informing consumers that avoiding phishing can reduce the risk of becoming a victim of identity theft may be more effective than merely promoting anti-phishing messages. A few panelists suggested that reminding consumers that phishers are looking for their own financial gain could be another effective message.

b. Developing behavioral messages

Participants indicated that the best anti-phishing messages are behavioral rather than technical. For example, instructions about how to check if a URL is bogus are not likely to be as effective as behavioral messages that might focus on encouraging users to learn to consider the source of the request before they give out their information. Evaluating who to trust on the Internet can help prevent users from becoming victims of phishing. It was noted that phishers use urgency and cause consumers to panic to elicit a quick emotional response from consumers. An educational message that might modify consumers' behavior in this scenario would be one that reminds consumers to take their time before giving out personal information, to be skeptical, and not to presume that all requests for information are safe. Participants described this as developing a healthy sense of skepticism — or "street smarts" — on the Internet. Considering that many online users are used to clicking quickly through links and are not necessarily technologically savvy,

panelists suggested that a catch phrase such as "stop, think, and verify" before responding to an email that asks for personal information is needed to raise awareness of phishing.

Participants also stated that messages to young people (and others) should focus on behaviors rather than technologies. That is, we should teach computer users to value their personal information more than they currently do and how to decide when to trust a request for it, rather than focus on a specific technology, such as email.

c. **Working together on a coalition**

Several participants suggested that refining anti-phishing messages requires input from the relevant stakeholders. This process should be informed by a holistic research approach — using academic research and industry information about user behavior and consumer surveys to get "test messages" before launching a national campaign. In general, participants at the roundtable concurred that a task force on phishing education is a good idea because many effective campaigns are developed by coalitions of business, government, and consumer organizations. Most attendees agreed to be on this task force.

2. **Strategies for Reaching the Right People at the Right Time and at the Right Place**

The group agreed that it is important to identify relevant "teachable moments" when consumers are more likely to be open to anti-phishing educational messages. Several tactics were discussed. Among them were:

a. **Educational landing pages**

As soon as phishing sites are removed by the ISPs they should be replaced by landing pages with appropriate educational messages about phishing. These educational pages would feature clear and simple anti-phishing messages, the consequences of giving up personal information, and information about where the consumer can get more information. For these educational landing

pages to be meaningful, they have to be up and running as quickly as possible once phishing pages are discovered so that if a consumer responds to what turns out to be a phishing email, the new landing page appears in place of the spoof site. The Anti-Phishing Working Group developed two versions of these educational landing pages in collaboration with Carnegie Mellon University and presented them to the roundtable participants. Participants believed that they were a good start, but recommended that more work be done, particularly to make the pages more concise, easier to understand, and more generic so that many organizations can use them.

b. **Using new communication channels to teach online safety**

Participants stressed the importance of using new channels to teach online safety. All of the break-out groups discussed the role of schools in educating young people about safe online behavior, and there was consensus that more school-based education on computer security, cyber safety, and cyber ethics is a good idea. Several participants pointed to the Virginia school system's legislatively-mandated Internet safety education program as an example.[3]

Panelists noted that anti-phishing messages to young computer users should be delivered through channels most young people use, for example, mobile devices, games, and videos, and should not be focused on email or specific technology.

Most participants believed that October, which the National Cyber Security Alliance promotes as Cyber Security Awareness Month, is a good time for all major stakeholders to focus on anti-phishing education and online safety. The group wants to explore ways to get more information about online safety to new computer users, including, for example, consumers who have just bought a new computer, or an operating system, or who have recently contracted with a

[3] *See* http://www.doe.virginia.gov/VDOE/Technology/OET/internet-safety-guidelines.shtml.

new ISP. Some participants noted that people favor security "checklists" with actions to take — or to avoid — to stay safe online; thus, a general checklist with anti-phishing messages may be part of a package of effective anti-phishing tools. Finally, there was some discussion that consumers would benefit from consistent anti-phishing software tools, such as online safety warnings and icons.

3. Developing Guidance for Businesses

In general, the group agreed that more information should be available for businesses on the impact of phishing and possible responses to a phishing attack. This guidance was described as a hybrid educational approach because it would include educating businesses as well as registrars and ISPs.

a. Educating small- and medium-sized enterprises

Small- and medium-sized enterprises were identified as vulnerable because they may lack the know-how to handle phishing attacks and communicate with customers effectively. These enterprises would benefit from data on the possible impact on their brand and from guidance on how to create a plan in case they are phished. Such guidance should include: how to communicate with consumers about phishing; how to work with ISPs, registrars, and security companies to take down spoofed sites; and how to post educational landing pages.[4]

b. Working with registrars and ISPs

It was noted that registrars and ISPs also should be encouraged to create a plan of action when they find out they are hosting a phishing site. Some participants suggested that a uniform

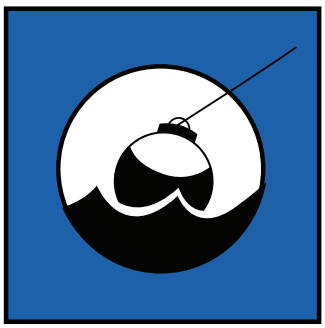
[4] A few participants mentioned "vishing," which is the use of social engineering and Voice over Internet Protocol technology ("VoIP") to gain access to private personal and financial information from consumers. Vishing is possible because VoIP technology allows for caller ID spoofing, which enables the "visher" to act anonymously. A few participants suggested using anti-vishing voice-mail messages to educate consumers about vishing when they call phone numbers used in vishing scams.

educational kit for registrars and ISPs be created. However, many noted that ISPs face international barriers and that it is difficult for them to work with foreign counterparts, both of which pose challenges to the implementation of such a plan.

IV. Conclusion

The workshop brought together a group of people who can play important roles in educating consumers and businesses about phishing practices and their impact. Feedback on the workshop was very positive, and plans are underway to continue the conversation in a meaningful way.

Appendix A



FTC Roundtable on Phishing Education

AGENDA

April 1, 2008

8:30am **Coffee and Networking**

9:00am **Welcoming Remarks**
Lydia Parnes, Director, Bureau of Consumer Protection, Federal Trade Commission

Agenda Overview and Introductions
Carolyn Shanoff, Associate Director, Division of Consumer and Business Education, Federal Trade Commission

Lois Greisman, Associate Director, Division of Marketing Practices, Federal Trade Commission

9:15am **Guided Discussion: Problem Overview**
Moderator: Sana Chriss, Federal Trade Commission

9:40am **Guided Discussion: Current Efforts to Fight Phishing Attacks and Educate Consumers**
Moderator: Rosario Méndez, Federal Trade Commission

10:15am **FTC Phishing Videos**

10:25am **BREAK**

10:40am **Guided Discussion: Other Examples of Current Efforts to Educate, Report and Alert**
Moderator: Nat Wood, Federal Trade Commission

11:15am **Working Session: Developing a Plan to Increase Consumer Education and Mobilize Key Players**
Moderators: Nat Wood, Jennifer Leach, Ethan Arenson, Sana Chriss, Rosario Méndez, Federal Trade Commission
(break into small groups)

12:15pm **BREAK**

12:30pm **Reports from the Working Session and Discussion**
Moderator: Nat Wood, Federal Trade Commission

12:55pm **Concluding Remarks**
Lois Greisman, Associate Director, Division of Marketing Practices, Federal Trade Commission

FEDERAL TRADE COMMISSION	ftc.gov
1-877-FTC-HELP	FOR THE CONSUMER